

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-89669

(P2000-89669A)

(43)公開日 平成12年3月31日(2000.3.31)

(51)Int.Cl.⁷

G 0 9 C 1/00

識別記号

6 2 0

F I

G 0 9 C 1/00

マークト* (参考)

6 2 0 Z

審査請求 未請求 請求項の数10 O L (全 8 頁)

(21)出願番号

特願平10-262037

(22)出願日

平成10年9月16日(1998.9.16)

(71)出願人 000006297

村田機械株式会社

京都府京都市南区吉祥院南落合町3番地

(71)出願人 597008636

笠原 正雄

大阪府箕面市栗生外院4丁目15番3号

(72)発明者 笠原 正雄

大阪府箕面市栗生外院4丁目15番3号

(72)発明者 村上 恭通

京都府京都市伏見区竹田向代町136番地

村田機械株式会社本社工場内

(74)代理人 100078868

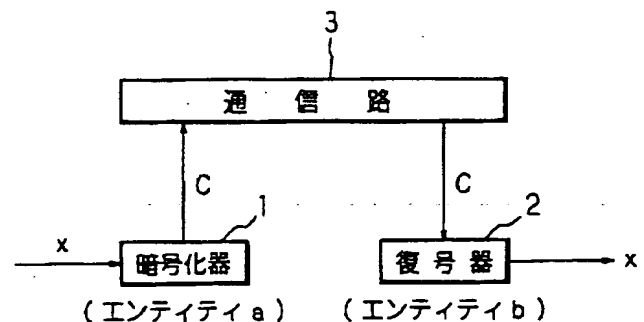
弁理士 河野 登夫

(54)【発明の名称】 暗号化方法、復号方法、暗号化・復号方法及び暗号通信システム

(57)【要約】

【課題】 高速の復号が可能な積和型暗号の暗号化・復号方法を提供する。

【解決手段】 平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $D = (D_0, D_1, \dots, D_{K-1})$ とを用いた内積により暗号文 $C = m_0 D_0 + m_1 D_1 + \dots + m_{K-1} D_{K-1}$ を得る積和型の暗号方式であつて、 D_i ($0 \leq i \leq K-1$)を $D_i = d / d_i$ (但し、 $d = d_0 d_1 \dots d_{K-1}$ (任意の2つの数 d_i, d_j は互いに素))に設定する。



BEST AVAILABLE COPY

【特許請求の範囲】

【請求項1】 平文をK分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $D = (D_0, D_1, \dots, D_{K-1})$ とを用いて暗号文 $C = m_0 D_0 + m_1 D_1 + \dots + m_{K-1} D_{K-1}$ を得る暗号化方法において、前記 D_i ($0 \leq i \leq K-1$)を $D_i = d / d_i$ (但し、 $d = d_0 d_1 \dots d_{K-1}$ (任意の2つの数 d_i, d_j は互いに素))に設定することを特徴とする暗号化方法。

【請求項2】 平文をK分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $D = (D_0, D_1, \dots, D_{K-1})$ とを用いて暗号文 $C = m_0 D_0 + m_1 D_1 + \dots + m_{K-1} D_{K-1}$ を得る暗号化方法において、前記 D_i ($0 \leq i \leq K-1$)を $D_i = (d / d_i) \cdot v_i$ (但し、 $d = d_0 d_1 \dots d_{K-1}$ (任意の2つの数 d_i, d_j は互いに素)、 v_i :乱数)に設定することを特徴とする暗号化方法。

【請求項3】 乱数ベクトル $v = (v_0, v_1, \dots, v_{K-1})$ を用いて暗号文 $C = m_0 v_0 D_0 + m_1 v_1 D_1 + \dots + m_{K-1} v_{K-1} D_{K-1}$ を得る請求項1記載の暗号化方法。

【請求項4】 請求項1, 2または3によって暗号化さ

$$C = m_0 c_0 + m_1 c_1 + \dots + m_{K-1} c_{K-1} \quad \dots (c)$$

暗号文Cに対して、中間復号文Mを式(d)のようにして求めるステップと、

$$M \equiv w^{-1} C \pmod{P} \quad \dots (d)$$

この中間復号文Mを以下の式(e)により復号して平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求めるステップと

$$m_i \equiv M D_i^{-1} \pmod{d_i} \quad \dots (e)$$

を有することを特徴とする暗号化・復号方法。

【請求項7】 平文をK分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $D = (D_0, D_1, \dots, D_{K-1})$ とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、

$$C = m_0 c_0 + m_1 c_1 + \dots + m_{K-1} c_{K-1} \quad \dots (h)$$

暗号文Cに対して、中間復号文Mを式(i)のようにして求めるステップと、

$$M \equiv w^{-1} C \pmod{P} \quad \dots (i)$$

この中間復号文Mを以下の式(j)により復号して平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求めるステップと

$$m_i \equiv M D_i^{-1} \pmod{d_i} \quad \dots (j)$$

を有することを特徴とする暗号化・復号方法。

【請求項8】 平文をK分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $D = (D_0, D_1, \dots, D_{K-1})$ とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、

*れた暗号文Cを復号する復号方法であって、以下の式

(a)により平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求めることを特徴とする復号方法。

$$m_i \equiv C D_i^{-1} \pmod{d_i} \quad \dots (a)$$

【請求項5】 前記K個の d_i の集合を複数組準備し、それぞれの集合毎に暗号文を得るようにした請求項1または2記載の暗号化方法。

【請求項6】 平文をK分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $D = (D_0, D_1, \dots, D_{K-1})$ とを用いて前記平文を暗号文に変換し、その暗号文を元の平文に変換する暗号化・復号方法において、

前記 D_i ($0 \leq i \leq K-1$)を整数 d_i を用いて d / d_i (但し、 $d = d_0 d_1 \dots d_{K-1}$ (任意の2つの数 d_i, d_j は互いに素))に設定するステップと、

$w < P$ (P :素数)を満たす w を選択し、式(b)により公開鍵ベクトル $c = (c_0, c_1, \dots, c_{K-1})$ を求めるステップと、

$$c_i \equiv w D_i \pmod{P} \quad \dots (b)$$

平文ベクトル m と公開鍵ベクトル c との内積により、式(c)に示す暗号文Cを作成するステップと、

*前記 D_i ($0 \leq i \leq K-1$)を式(f)にて設定するステップと、

$$D_i = (d / d_i) \cdot v_i \quad \dots (f)$$

但し、 v_i :乱数

d_i :整数

$$d = d_0 d_1 \dots d_{K-1}$$

30 (任意の2つの整数 d_i, d_j は互いに素)

$w < P$ (P :素数)を満たす w を選択し、式(g)により公開鍵ベクトル $c = (c_0, c_1, \dots, c_{K-1})$ を求めるステップと、

$$c_i \equiv w D_i \pmod{P} \quad \dots (g)$$

平文ベクトル m と公開鍵ベクトル c との内積により、式(h)に示す暗号文Cを作成するステップと、

※

素数 P, Q を設定するステップと、

基数ベクトル D_{P_i} ($0 \leq i \leq K-1$)を整数 d_{P_i} を用いて $D_{P_i} = d_P / d_{P_i}$ (但し、 $d_P = d_{P_0} d_{P_1} \dots d_{P_{K-1}}$ (任意の2つの数 d_{P_i}, d_{P_j} は互いに素))に設定するステップと、

40

基数ベクトル D_{Q_i} ($0 \leq i \leq K-1$)を整数 d_{Q_i} を用いて $D_{Q_i} = d_Q / d_{Q_i}$ (但し、 $d_Q = d_{Q_0} d_{Q_1} \dots d_{Q_{K-1}}$ (任意の2つの数 d_{Q_i}, d_{Q_j} は互いに素))に設定するステップと、

中国人の剰余定理を用いて、 P, Q による余りがそれぞれ D_{P_i}, D_{Q_i} となるような最小の整数 D_i を導くステップと、

50

$w < N$ ($N = P Q$)を満たす w を選択し、式(k)によ

り公開鍵ベクトル $c = (c_0, c_1, \dots, c_{K-1})$ を求めるステップと、

$$c_i \equiv w D_i \pmod{N} \quad \dots (k) \quad *$$

$$C = m_0 c_0 + m_1 c_1 + \dots + m_{K-1} c_{K-1} \quad \dots (1)$$

暗号文 C に対して、法 P 、法 Q において、それぞれ中間復号文 M_P 、 M_Q を式 (m)、式 (n) のようにして求めるステップと、

$$M_P \equiv w^{-1} C \pmod{P} \quad \dots (m)$$

$$M_Q \equiv w^{-1} C \pmod{Q} \quad \dots (n)$$

この中間復号文 M_P 、 M_Q を以下の式 (o)、式 (p) により復号して余りのペア $(m_i^{(P)}, m_i^{(Q)})$ を求めるステップと、

$$m_i^{(P)} \equiv M_P D_{Pi}^{-1} \pmod{d_{Pi}} \quad \dots (o)$$

$$m_i^{(Q)} \equiv M_Q D_{Qi}^{-1} \pmod{d_{Qi}} \quad \dots (p)$$

求めた $m_i^{(P)}$ 、 $m_i^{(Q)}$ に中国人の剰余定理を適用して、平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求めるステップとを有することを特徴とする暗号化・復号方法。

【請求項9】 前記 N を法として前記暗号文 C を送るようにした請求項8記載の暗号化・復号方法。

【請求項10】 複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項1、2、3または5の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文を元の平文に復号する復号器とを備えることを特徴とする暗号通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、平文を暗号文に変換するための暗号化方法、及び、暗号文を元の平文に変換するための復号方法に関し、特に、積和型暗号に関する。

【0002】

【従来の技術】 高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複製が可能である、複製物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」、「マルチアクセス」、「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

【0003】 暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号にお

* 平文ベクトル m と公開鍵ベクトル c との内積により、式 (1) に示す暗号文 C を作成するステップと、

いて、誰でも理解できる元の文 (平文) を第三者には意味がわからない文 (暗号文) に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【0004】 暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を元に平文に復号する。

【0005】 これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵によって変換された暗号文は秘密鍵でのみ復号することができる。

【0006】

【発明が解決しようとする課題】 公開鍵暗号系の1つである積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。

【0007】 本発明は斯かる事情に鑑みてなされたものであり、高速な復号処理が可能である、積和型暗号に関する新規の暗号化方法及び復号方法を提供することを目的とする。

【0008】

【課題を解決するための手段】 請求項1に係る暗号化方法は、平文を K 分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $D = (D_0, D_1, \dots, D_{K-1})$ とを用いて暗号文 $C = m_0 D_0 + m_1 D_1 + \dots + m_{K-1} D_{K-1}$ を得る暗号化方法において、前記 D_i ($0 \leq i \leq K-1$) を $D_i = d / d_i$ (但し、 $d = d_0 d_1 \dots d_{K-1}$ (任意の2つの数 d_i, d_j は互いに素)) に設定することを特徴とする。

【0009】 請求項2に係る暗号化方法は、平文を K 分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $D = (D_0, D_1, \dots, D_{K-1})$ とを用い

10

20

30

40

50

て暗号文 $C = m_0 D_0 + m_1 D_1 + \dots + m_{K-1} D_{K-1}$ を得る暗号化方法において、前記 D_i ($0 \leq i \leq K-1$) を $D_i = (d/d_i) \cdot v_i$ (但し、 $d = d_0 d_1 \dots d_{K-1}$ (任意の2つの数 d_i, d_j は互いに素), v_i : 乱数) に設定することを特徴とする。

【0010】請求項3に係る暗号化方法は、請求項1において、乱数ベクトル $v = (v_0, v_1, \dots, v_{K-1})$ を用いて暗号文 $C = m_0 v_0 D_0 + m_1 v_1 D_1 + \dots + m_{K-1} v_{K-1} D_{K-1}$ を得ることを特徴とする。

【0011】請求項4に係る復号方法は、請求項1, 2 または3の何れかによって暗号化された暗号文 C を復号する復号方法であって、以下の式 (a) により平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求めることを特徴とする。

$$m_i \equiv C D_i^{-1} \pmod{d_i} \quad \dots (a)$$

【0012】請求項5に係る暗号化方法は、請求項1または2において、前記 K 個の d_i の集合を複数組準備 *

$$C = m_0 c_0 + m_1 c_1 + \dots + m_{K-1} c_{K-1} \quad \dots (c)$$

暗号文 C に対して、中間復号文 M を式 (d) のようにして求めるステップと、

$$M \equiv w^{-1} C \pmod{P} \quad \dots (d)$$

この中間復号文 M を以下の式 (e) により復号して平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求めるステップと

$$m_i \equiv M D_i^{-1} \pmod{d_i} \quad \dots (e)$$

を有することを特徴とする。

【0014】請求項7に係る暗号化・復号方法は、平文を K 分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $D = (D_0, D_1, \dots, D_{K-1})$ とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、

$$C = m_0 c_0 + m_1 c_1 + \dots + m_{K-1} c_{K-1} \quad \dots (h)$$

暗号文 C に対して、中間復号文 M を式 (i) のようにして求めるステップと、

$$M \equiv w^{-1} C \pmod{P} \quad \dots (i)$$

この中間復号文 M を以下の式 (j) により復号して平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求めるステップと

$$m_i \equiv M D_i^{-1} \pmod{d_i} \quad \dots (j)$$

を有することを特徴とする。

【0015】請求項8に係る暗号化・復号方法は、平文を K 分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $D = (D_0, D_1, \dots, D_{K-1})$ とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、素数 P, Q を設定するステップと、基数ベクトル D_{P_i} ($0 \leq i \leq K$ ★

$$C = m_0 c_0 + m_1 c_1 + \dots + m_{K-1} c_{K-1} \quad \dots (l)$$

暗号文 C に対して、法 P , 法 Q において、それぞれ中間復号文 M_P, M_Q を式 (m), 式 (n) のようにして求めるステップと、

*し、それぞれの集合毎に暗号文を得るようにしたことを特徴とする。

【0013】請求項6に係る暗号化・復号方法は、平文を K 分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $D = (D_0, D_1, \dots, D_{K-1})$ とを用いて前記平文を暗号文に変換し、その暗号文を元の平文に変換する暗号化・復号方法において、前記 D_i ($0 \leq i \leq K-1$) を整数 d_i を用いて d/d_i (但し、 $d = d_0 d_1 \dots d_{K-1}$ (任意の2つの数 d_i, d_j は互いに素)) に設定するステップと、 $w < P$ (P : 素数) を満たす w を選択し、式 (b) により公開鍵ベクトル $c = (c_0, c_1, \dots, c_{K-1})$ を求めるステップと、

$$c_i \equiv w D_i \pmod{P} \quad \dots (b)$$

平文ベクトル m と公開鍵ベクトル c との内積により、式 (c) に示す暗号文 C を作成するステップと、

※前記 D_i ($0 \leq i \leq K-1$) を式 (f) にて設定するステップと、

$$D_i = (d/d_i) \cdot v_i \quad \dots (f)$$

但し、 v_i : 乱数

d_i : 整数

$$d = d_0 d_1 \dots d_{K-1}$$

(任意の2つの整数 d_i, d_j は互いに素)

$w < P$ (P : 素数) を満たす w を選択し、式 (g) により公開鍵ベクトル $c = (c_0, c_1, \dots, c_{K-1})$ を求めるステップと、

$$c_i \equiv w D_i \pmod{P} \quad \dots (g)$$

平文ベクトル m と公開鍵ベクトル c との内積により、式 (h) に示す暗号文 C を作成するステップと、

★ $K-1$) を整数 d_{P_i} を用いて $D_{P_i} = d_P / d_{P_i}$ (但し、 $d_P = d_{P_0} d_{P_1} \dots d_{P_{K-1}}$ (任意の2つの数 d_{P_i}, d_{P_j} は互いに素)) に設定するステップと、基数ベクトル D_{Q_i} ($0 \leq i \leq K-1$) を整数 d_{Q_i} を用いて $D_{Q_i} = d_Q / d_{Q_i}$ (但し、 $d_Q = d_{Q_0} d_{Q_1} \dots d_{Q_{K-1}}$ (任意の2つの数 d_{Q_i}, d_{Q_j} は互いに素)) に設定するステップと、中国剰余定理を用いて、 P, Q による余りがそれぞれ

40 D_{P_i}, D_{Q_i} となるような最小の整数 D_i を導くステップと、 $w < N$ ($N = PQ$) を満たす w を選択し、式 (k) により公開鍵ベクトル $c = (c_0, c_1, \dots, c_{K-1})$ を求めるステップと、

$$c_i \equiv w D_i \pmod{N} \quad \dots (k)$$

平文ベクトル m と公開鍵ベクトル c との内積により、式 (l) に示す暗号文 C を作成するステップと、

$$M_P \equiv w^{-1} C \pmod{P} \quad \dots (m)$$

$$M_Q \equiv w^{-1} C \pmod{Q} \quad \dots (n)$$

50 この中間復号文 M_P, M_Q を以下の式 (o), 式 (p)

により復号して余りのペア ($m_i^{(P)}$, $m_i^{(Q)}$) を求めるステップと、

$$m_i^{(P)} \equiv M_P D_{P_i}^{-1} \pmod{d_{P_i}} \quad \dots (o)$$

$$m_i^{(Q)} \equiv M_Q D_{Q_i}^{-1} \pmod{d_{Q_i}} \quad \dots (p)$$

求めた $m_i^{(P)}$, $m_i^{(Q)}$ に中国人の剰余定理を適用して、平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求めるステップとを有することを特徴とする。

【0016】請求項9に係る暗号化・復号方法は、請求項8において、前記Nを法として前記暗号文Cを送るようにしたことを特徴とする。

【0017】請求項10に係る暗号通信システムは、複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項1, 2, 3または5の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから*

$$M = m_0 D_0 + m_1 D_1 + \dots + m_{K-1} D_{K-1} \quad \dots (3)$$

但し、メッセージベクトル m の各要素 m_i は $m_i < d_i$ を満たすように設定する。

【0020】本発明では、このようにして、つまり、式(1)～式(3)を利用して、暗号文を作成する。

【0021】基数を式(2)で与えた場合には、以下に示すアルゴリズムにより、整数Mからメッセージ $m = (m_0, m_1, \dots, m_{K-1})$ を復号することができる。この復号アルゴリズムを並列復号アルゴリズムという。

【0022】〔並列復号アルゴリズム〕

unit i (m_i の復号)

$$m_i \equiv M D_i^{-1} \pmod{d_i}$$

【0023】このような概念に基づく暗号化手法とそれに対する復号方法とを、本発明の特徴とする。なお、具体的な手法については後述する。

【0024】

【発明の実施の形態】以下、本発明の実施の形態について具体的に説明する。図1は、本発明による暗号化方法・復号方法をエンティティa, b間の情報通信に利用した状態を示す模式図である。図1の例では、一方のエンティティaが、暗号化器1にて平文xを暗号文Cに暗号化し、通信路3を介してその暗号文Cを他方のエンティティbへ送信し、エンティティbが、復号器2にてその暗号文Cを元の平文xに復号する場合を示している。 ※

$$C = m_0 c_0 + m_1 c_1 + \dots + m_{K-1} c_{K-1} \quad \dots (6)$$

【0027】エンティティb側では、以下のようにして復号処理が行われる。最初に、暗号文Cに対して、中間復号文Mを式(7)のようにして導く。

$$M \equiv w^{-1} C \pmod{P} \quad \dots (7)$$

【0028】この中間復号文Mは、具体的には前記式(3)として与えられるので、前述の並列復号アルゴリズムによって復号できる。K重の並列処理が可能である場合には、2回の乗除算処理を実行するのに必要な時間で暗号文Cを高速に復号できる。また、本発明では、最上位の桁から順に(または最下位の桁から順に)メッセ

*ら他方のエンティティへ送信する通信路と、送信された暗号文を元の平文に復号する復号器とを備えることを特徴とする。

【0018】本発明の暗号化方法・復号方法の概念について、以下に説明する。K個の整数を要素とする集合 $\{d_i\}$ を考える。なお、この集合の任意の2つの要素は互いに素である。そして、式(1)に示すように、これらのK個の要素の積をdとし、基数 D_i を式(2)のように定義する。

$$d = d_0 d_1 \dots d_{K-1} \quad \dots (1)$$

$$D_i = d / d_i \quad \dots (2)$$

【0019】そして、メッセージ $m = (m_0, m_1, \dots, m_{K-1})$ を、基数 $D = (D_0, D_1, \dots, D_{K-1})$ を用いて、下記式(3)に示すように表記する。

※【0025】(第1実施の形態) 秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵: $\{d_i\}$, P, w

20 ・公開鍵: $\{c_i\}$

前記式(2)のように基数を与える。この場合、基数ベクトル $\{D_i\}$ は超増加数列ではなく、LLL (Lenstra-Lenstra-Lovasz) 法攻撃に強い。また、 $w < P$ (Pは大きな素数) を満たす整数wをランダムに選ぶ。また、メッセージベクトル m の各要素 m_i は $m_i < d_i$ を満たすように設定する。整数wを用いてDの成分より、公開鍵ベクトル c を式(4), (5)のように導く。

$$c_i \equiv w D_i \pmod{P} \quad \dots (4)$$

$$c = (c_0, c_1, \dots, c_{K-1}) \quad \dots (5)$$

30 【0026】また、 $\mu < \min(d_0, d_1, \dots, d_{K-1})$ なる μ が各エンティティに公開される。エンティティa側で、この公開された μ に基づいて、K次元の μ 以下の大きさのメッセージベクトルに平文xを分割する。エンティティa側で、メッセージベクトル m と公開鍵ベクトル c との内積を式(6)のように求めて、平文xを暗号化して暗号文Cを得る。作成された暗号文Cは通信路3を介してエンティティaからエンティティbへ送信される。

ーじベクトルの各要素を復号する必要はなく、任意の桁のメッセージ要素を自由に並列的に復号できるので、並列通信が可能となる。

【0029】ところで、2つの d_i, d_j の組 (d_i, d_j) を総当たりに仮定すると、Pが露呈することになる。よって、実用上 d_i は 2^{32} 程度に選ぶ必要がある。

【0030】ここで、第1実施の形態における具体例を示す。

50 ・秘密鍵

$d = (11, 17, 29)$

$D = (17 \cdot 29, 29 \cdot 11, 11 \cdot 17)$

$= (493, 319, 187)$

$P = 59659$

$w = 25252$

$w^{-1} \equiv 48633 \pmod{P}$

(D_1, D_2, D_3 は超増加数列でない)

・公開鍵

$c \equiv wD \pmod{P}$

・暗号化

メッセージを $m = (4, 6, 8)$ とする。

$C = c \cdot m = 241698$

・復号

中間復号文 M を求め、並列復号アルゴリズムを用いて復号する。

$M \equiv w^{-1}C \equiv 5382 \pmod{59659}$

$m_0 \equiv 5382 \cdot 493^{-1} \equiv 4 \pmod{11}$

$m_1 \equiv 5382 \cdot 319^{-1} \equiv 6 \pmod{17}$

$m_2 \equiv 5382 \cdot 187^{-1} \equiv 8 \pmod{29}$

以上のようにして、メッセージ $m = (4, 6, 8)$ を得る。

【0031】(第2実施の形態)第1実施の形態に乱数を付加した第2実施の形態について説明する。第1実施の形態において、 w と D_i との積の総乗積を求めると、下記式(8)のようになって w と d との多重積となるので、 w, d が求まる可能性が皆無とは言えない。よって、第2実施の形態では、第1実施の形態での基数ベクトルに乱数を掛け合わせたものを基数ベクトルとして使用することにより安全性を強化する。

【0032】

【数1】

$$\prod_{i=0}^{K-1} w D_i = w^K \cdot \frac{d^K}{d} = w^K d^{K-1} \quad \dots (8)$$

【0033】秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵: $\{d_i\}, \{v_i\}, P, w$

・公開鍵: $\{c_i\}$

同程度の大きさの乱数 v_0, v_1, \dots, v_{K-1} を用いて、基数 D_i を式(9)のように与える。但し、 d_i と v_i とは互いに素であるとする。

$D_i = (d/d_i) \cdot v_i \quad \dots (9)$

【0034】整数 w を用いて、第1実施の形態と同様に、公開鍵ベクトル c を以下の式(10)、式(11)のように求める。

$c_i \equiv w D_i \pmod{P} \quad \dots (10)$

$c = (c_0, c_1, \dots, c_{K-1}) \quad \dots (11)$

【0035】メッセージベクトル m と公開鍵ベクトル c との内積により、第1実施の形態と同様に(前記式

(6))、暗号文 C を得る。

【0036】復号処理は、以下のようにして行われる。暗号文 C に対して、中間復号文 M を式(12)のようにして求める。

$M \equiv w^{-1}C \pmod{P} \quad \dots (12)$

この中間復号文 M は、具体的には前記式(3)として与えられるので、第1実施の形態と同様に、並列復号アルゴリズムによって復号される。

【0037】ここで、第2実施の形態における具体例を示す。

・秘密鍵

$d = (11, 17, 29)$

$v = (8, 7, 5)$

$D = (2465, 2233, 1496)$

$P = 59659$

$w = 25252$

$w^{-1} \equiv 48633 \pmod{P}$

・公開鍵

$c \equiv wD$

$\equiv (21843, 9961, 12845) \pmod{P}$

・暗号化

メッセージを $m = (7, 8, 9)$ とする。

$C = c \cdot m$

$= 348194$

・復号

中間復号文 M を求め、並列復号アルゴリズムを用いて復号する。

$M \equiv w^{-1}C \equiv 48583 \pmod{59659}$

$m_0 \equiv 48583 \cdot 2465^{-1} \equiv 7 \pmod{11}$

$m_1 \equiv 48583 \cdot 2233^{-1} \equiv 8 \pmod{17}$

$m_2 \equiv 48583 \cdot 1496^{-1} \equiv 9 \pmod{29}$

以上のようにして、メッセージ $m = (7, 8, 9)$ を得る。

【0038】(第3実施の形態)第2実施の形態では、基数ベクトル自体に乱数を組み込むようにしたが、第1実施の形態と同じ基数ベクトルを使用し、暗号文 C を作成する段階で乱数 v_0, v_1, \dots, v_{K-1} を付加することもできる。この場合の暗号文 C は、第2実施の形態と同じ形となる。

【0039】(第4実施の形態)第1実施の形態で基数ベクトルを多重化した第4実施の形態について説明する。第4実施の形態は、第1実施の形態による基数ベクトル $\{D_i\}$ を2つの法それぞれにおいて設定し、中国人の剰余定理を利用した暗号化・復号方法である。

【0040】秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵: $\{d_{P_i}\}, \{d_{Q_i}\}, P, Q, N, w$

・公開鍵: $\{c_i\}$

2つの大きな素数 P, Q を選択し、それらの積を N とする。第1実施の形態における K 個の要素からなる集合

$\{d_i\}$ を2通り準備し、 $\{d_{P_i}\}$ 、 $\{d_{Q_i}\}$ とする。
また、それらより生成した基数を $\{D_{P_i}\}$ 、 $\{D_{Q_i}\}$ とする。中国人の剰余定理を用いて、 P 、 Q による余りがそれぞれ D_{P_i} 、 D_{Q_i} となるような最小の整数 D_i を導き、それを基数とする。

【0041】 N を法として、秘密の乱数 w を用いて、第1実施の形態と同様に、公開鍵ベクトル c を以下の式 (13)、式 (14) のように求める。

$$c_i \equiv w D_i \pmod{N} \quad \dots (13)$$

$$c = (c_0, c_1, \dots, c_{K-1}) \quad \dots (14)$$

【0042】メッセージベクトル m と公開鍵ベクトル c *

$$M_P = m_0^{(P)} D_{P0} + m_1^{(P)} D_{P1} + \dots + m_{K-1}^{(P)} D_{PK-1} \quad \dots (17)$$

$$M_Q = m_0^{(Q)} D_{Q0} + m_1^{(Q)} D_{Q1} + \dots + m_{K-1}^{(Q)} D_{QK-1} \quad \dots (18)$$

$$m_i \equiv m_i^{(P)} \pmod{d_{P_i}} \quad \dots (19)$$

$$m_i \equiv m_i^{(Q)} \pmod{d_{Q_i}} \quad \dots (20)$$

【0045】 M_P 、 M_Q に対して、並列復号アルゴリズムを適用することによって、余りのペア $(m_i^{(P)}, m_i^{(Q)})$ を導くことができる。これらに対して中国人の剰余定理を適用すると、メッセージ $m_i < l_{cm}$ (d_{P_i} 、 d_{Q_i}) を復号することができる。

【0046】ここで、第4実施の形態における具体例を示す。

・秘密鍵

$$d_P = (11, 17, 29)$$

$$d_Q = (13, 19, 23)$$

$$D_P = (493, 319, 187)$$

$$D_Q = (437, 299, 247)$$

$$D = (946872238594, 409641492482, 772314923252)$$

$$P = 1042183$$

$$Q = 960119$$

$$N = 1000619699777$$

$$w = 947284758293$$

$$w^{-1} \equiv 337608855274 \pmod{N}$$

・公開鍵

$$c \equiv w D \equiv (940952460514, 717925054865, 8707125634) \pmod{N}$$

・暗号化

メッセージを $m = (45, 67, 89)$ とする。

$$C = c \cdot m = 167937257544978$$

・復号

中間復号文 M_P 、 M_Q を求め、並列復号アルゴリズムを用いる。

$$M_P \equiv w^{-1} C \equiv 60201 \pmod{1042183}$$

$$M_Q \equiv w^{-1} C \equiv 61681 \pmod{960119}$$

$$m_0^{(P)} \equiv M_P \cdot 493^{-1} \equiv 1 \pmod{11}$$

$$m_1^{(P)} \equiv M_P \cdot 319^{-1} \equiv 16 \pmod{17}$$

$$m_2^{(P)} \equiv M_P \cdot 187^{-1} \equiv 2 \pmod{29}$$

$$D_{P_j}$$

*との内積により、第1実施の形態と同様に (前記式 (6))、暗号文 C を得る。

【0043】復号処理は、以下のようにして行われる。暗号文 C に対して、法 P 、法 Q において、それぞれ中間復号文 M_P 、 M_Q を式 (15)、式 (16) のようにして導く。

$$M_P \equiv w^{-1} C \pmod{P} \quad \dots (15)$$

$$M_Q \equiv w^{-1} C \pmod{Q} \quad \dots (16)$$

【0044】各中間復号文 M_P 、 M_Q に関して、式 (17)、式 (18) が成立する。但し、 m_i は、式 (19)、式 (20) の何れかであるとする。

$$\ast m_0^{(Q)} \equiv M_Q \cdot 437^{-1} \equiv 6 \pmod{13}$$

$$m_1^{(Q)} \equiv M_Q \cdot 299^{-1} \equiv 10 \pmod{19}$$

$$20 \quad m_2^{(Q)} \equiv M_Q \cdot 247^{-1} \equiv 20 \pmod{23}$$

($m_0^{(P)}$ 、 $m_0^{(Q)}$) から中国人の剰余定理により、 $m_0 = 45$ を求める。同様に、($m_1^{(P)}$ 、 $m_1^{(Q)}$)、($m_2^{(P)}$ 、 $m_2^{(Q)}$) から $m_1 = 67$ 、 $m_2 = 89$ を求める。以下のようにして、メッセージ $m = (45, 67, 89)$ を得る。

【0047】なお、合成数 N を法とする第4実施の形態のような多重化方式では、 N の素因数分解が困難である場合、 N を公開しても安全と考えられる。よって、そのような場合には、 N を法として求めた暗号文 C を送付することにより、暗号化効率が向上する。

【0048】(第5実施の形態) 第5実施の形態は、第4実施の形態に乱数を付加した暗号方式、言い換えると、第2実施の形態で基数ベクトルを多重化した暗号方式である。なお、この第5実施の形態については、前述の第1～第4実施の形態を参照すれば容易にその内容が理解されるので、詳細な説明は省略する。

【0049】(第6実施の形態) 第4実施の形態では、2個の素数を用いた多重化方式について説明したが、3個以上の素数を用いて多重化するようにしても良い。第6実施の形態では L 個の素数 P_0 、 P_1 、 \dots 、 P_{L-1} を用いる場合について説明する。なお、 $P_0 = P$ 、 $P_1 = Q$ とすれば、第4実施の形態と一致する。

【0050】秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵: $\{P_j\}$ 、 $\{r_{j,i}\}$ 、 w

・公開鍵: $\{c_i\}$

素数 P_j ($j = 0, 1, \dots, L-1$) に対し、第4実施の形態における D_P 、 D_Q と同様なベクトル D_{P_j} を式 (21) のように与える。

※

13

$$= (r_j / r_{j,0}, r_j / r_{j,1}, \dots, r_j / r_{j,j}, \dots, r_j / r_{j,K-1})$$

14

... (21)

但し、 $r_j = r_{j,0} r_{j,1} \dots r_{j,K-1}$

【0051】ここで、中国人の剰余定理を適用することにより、式(22)のようになる最小の整数を D_i として、基数とする。

$$D_i \equiv D_{P_{j,i}} \pmod{P_j} \quad \dots (22)$$

そして、 $N = P_0 P_1 \dots P_{L-1}$ を法として、第1実施の形態と同様に公開鍵 c を準備する。

【0052】第6実施の形態では、第1実施の形態と比

$$D_{P_0} = (r_0 / r_{0,0}, r_0 / r_{0,1}, \dots, r_0 / r_{0,K-1})$$

... (23)

【0053】なお、この第6実施の形態において、 $r_{j,i}$ を16ビット程度、 $K=L=8$ とした場合、公開鍵サイズは約8.2 キロビット、秘密パラメータ数は74となる。

【0054】

【発明の効果】以上のように、本発明では、暗号化する際の基数 D_i を $\bar{D}_i = d / d_i$ (但し、 $d = d_0 d_1 \dots d_{K-1}$) に設定するようにしたので、平文ベクトルの各要素を並列的に復号でき、簡単な装置構成にて高速な復号を行うことができる。この結果、積和型暗号の実用化

べて、いわば2次元的な構造が組み込まれる。このことによって、次のような効果が期待される。

(1) $K=L$ とした場合、 K^2 個のパラメータを用いてはじめてメッセージが復号される。次元数 K を同一にして比較した場合、より安全なシステムになっている。

(2) 同様に $K=L$ とした場合、式(23)に示す D_{P_0} を j 回巡回置換したベクトルを D_{P_j} として用いると、回路の単純化が可能となる。

の道を開くことに、本発明は大いに寄与できる。

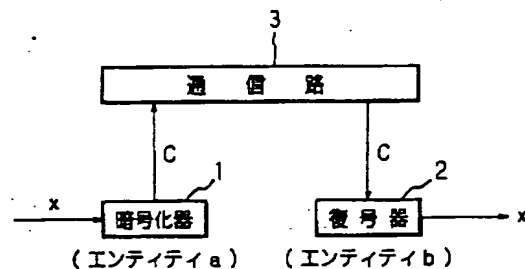
【図面の簡単な説明】

【図1】2人のエンティティ間における情報の通信状態を示す模式図である。

【符号の説明】

- 1 暗号化器
- 2 復号器
- 3 通信路
- a, b エンティティ

【図1】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.